Powers in clock arithmetic

$4^6 \equiv ? \mod 7$

$4^6 \equiv (4^2)^3 \equiv 2^3 \equiv 8 \equiv 1 \mod 7$

Let's try

$38^{75} \equiv ? \mod 103$

$38^{75} \equiv 38^{(64+8+2+1)} \mod 103$

$\equiv 38\,(38^2)(38^8)(38^{64}) \mod 103$

$\equiv 38 \cdot (2)(2^4)(2^{32}) \mod 103$

$\equiv 38 \cdot 2 \cdot 16 \cdot 16^8$

$\equiv 38 \cdot 2 \cdot 16 \cdot 50^4$

$\equiv 38 \cdot 2 \cdot 16 \cdot 63$

$\equiv 79$

Euler's Theorem

If a, m are integers with $\gcd(a,m) = 1$, then

$$a^{\phi(m)} \equiv 1 \mod m$$

Example $a = 4, \; m = 9$

$\phi(9) = 6$

$$a^{\phi(m)} = 4^6 \equiv (4^2)^3 \equiv 7^3 \equiv (-2)^3 \equiv -8 \equiv 1 \mod 9$$

Lemma Let d, e be integers with $d \equiv e^{-1} \mod \phi(n)$, with $n = pq$ where p, q are distinct primes. Let a be an integer with $\gcd(a,n) = 1$. Then

$$(a^e)^d \equiv a \mod n$$

Proof

$$(a^e)^d = a^{ed} = a^{1 + k\phi(n)}$$

$$= a\left(a^{\phi(n)}\right)^k$$

$$\equiv a \cdot 1 \mod n$$

$$\equiv a \mod n.$$

QED

Example Calculate $2^{1000000} \mod 77$.

$\phi(77) = \phi(7 \cdot 11) = \phi(7)\,\phi(11)$
$= 6 \cdot 10 = 60$

Soln

$$2^{1000000} = (2^{60})^{16666}\, 2^{40}$$
$$\equiv 1^{16666} \cdot 2^{40} \mod 77$$
$$\equiv 2^{40}$$
$$\vdots \leftarrow \text{some hard}$$
$$\equiv 23 \mod 77$$

Special case of Euler's Theorem

Fermat's Little Theorem

For a prime p and integer a not divisible by p, we have

$$a^{p-1} \equiv 1 \mod p$$

Proof of Fermat's Little Theorem

Let a, p be two integers as in the theorem.

Consider

$1.a,\ 2.a,\ 3.a,\ \dots,\ (p-1).a \mod p$

CLAIM: No two numbers in the green list are the same mod p.

Proof of claim

Suppose that two numbers in the list, say $i.a$ and $j.a$, were the same mod p.

Then

$$i.a \equiv j.a \mod p.$$

Then

$$i.a - j.a \equiv 0 \mod p$$

and

$$(i-j).a \equiv 0 \mod p.$$

So $(i-j).a$ is divisible by p.

Since a is not divisible by p we must have $(i-j)$ is divisible by p.

So $i-j \equiv 0 \mod p$

or $i \equiv j \mod p$.

This proves the claim. ∎

Now

$$(1.a)(2.a)(3.a)\cdots((p-1)a)$$
$$\equiv 1.2.3.\cdots(p-1)\,a^{p-1}$$
$$\equiv 1.2.3.\cdots(p-1) \mod p$$

Maths.

Hence $a^{p-1} \equiv 1 \mod p$.

QED